REMARKS

Claims 1, 3-30, and 32-81 are pending and remain. Claims 1, 79, 80, and 81 have been amended. No new matter has been entered.

The amendments present the rejected claims in better form for consideration on appeal and may be admitted pursuant to 37 C.F.R. § 1.116(b)(2).

Rejections under 35 U.S.C. § 101

Claims 1, 3-29, 60-68, and 79 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. A device, as claimed in Claims 1, 3-29, 60-68, and 79 is understood to be a piece of hardware. The claims have been amended per the Examiner's suggestions and are now statutory. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson and Griffiths

Claims 1, 3-10, 17-20, 27-30, 32-39, 46-49, 56-61, 68-70, 77, and 78 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 7,027,872, to Thompson, in view of U.S. Patent No. 7,136,999, to Griffiths ("Griffiths"). Applicant traverses.

The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness, which includes a clear articulation of the reasons or rationale why the claimed invention would have been obvious. MPEP 2142. Exemplary rationales to support a conclusion of obviousness are listed in MPEP 2143, although the list is not all-inclusive.

The claims appear to be rejected under the rationale outlining combining prior art elements according to known methods to yield predicable results, which includes *inter alia* "a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference." MPEP 2143(A). If any of the findings cannot be made, this rational cannot be used to support a conclusion that the claim would have been obvious. *Id.*

Thompson discloses a medical data management system for variable data encryption (Thompson, Col. 4, lines 40-44). A transmitting device receives data from an implantable medical device (Thompson, Col. 8, lines 20-26). Once received, a classifier determines a type of the data, which is then output to a segregator (Thompson, Col. 7, lines 14-16). The segregator separates the data based on predetermined security levels to determine what level of encryption, if necessary, is needed (Thompson, Col. 7, lines 17-20). A key source provides the transmitting device with an encryption key (Thompson, Col. 8, lines 48-50). Upon determining the level of encryption needed, the data is encrypted with the encryption key and transmitted to a receiving device (Thompson, Col. 7, Lines 23-30). The receiving device decrypts the data with a corresponding decryption key provided by the key source (Thompson, Col. 8, lines 48-50).

In contrast, Griffiths discloses a system and method for authenticating two electronic devices using Bluetooth. The two electronic devices initially authenticate over a short-range wireless link using a Bluetooth network in which a user has constrained access (Griffiths, Col. 3, lines 61-67). When one of the devices moves outside of the network boundary, the two electronic devices can still communicate if the initial authentication was successful (Griffiths, Col. 4, lines 16-19). To initiate communication, one of the devices, known as the slave device, establishes a link to the other device, known as the master device, over a "secondary" link (Griffiths, Col. 4, lines 21-24). Next, the master device offers to use the authentication protocol of the primary data link to facilitate device authentication by exchanging key information with the slave device (Griffiths, Col. 4, lines 28-36). If the key information matches, the master and slave devices are allowed to communicate over the "secondary" link (Griffiths, Col. 4, lines 37-39).

Together, Thompson and Griffiths fail to teach each and every element of the claims. Claim 1 recites a secure key repository configured to maintain a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session, wherein the secure key repository is at least one of a device or a module executed by a device. Claim 30 recites maintaining a

crypto key uniquely associated with an implantable medical device in a secure key repository to authenticate data during a data exchange session. Claim 59 recites means for maintaining a crypto key uniquely associated with an implantable medical device in a secure key repository to authenticate data during a data exchange session.

Applicant cannot find such limitations in Thompson. Thompson discloses a key source for providing a programmer and a clinician computer with corresponding encryption keys (Thompson, Col. 8, lines 48-50). Encrypted sensitive information is transferred from an implantable medical device to a programmer (Thompson, Col. 8, lines 20-26 and lines 37-41). The key source provides the programmer with an encryption key to encrypt the sensitive information for sending to the clinician computer (Thompson, Col. 8, lines 48-50; Col. 9, lines 10-12). A corresponding encryption key is provided to the clinician computer for decrypting the encrypted sensitive information, once received (Thompson, Col. 8, lines 48-50; Col. 10, lines 10-20). Thompson teaches providing corresponding encryption and decryption keys to the programmer and clinician computer. However, Thompson fails to specify that the corresponding encryption and decryption keys are specific to any one of the devices to which the key is provided. Thus, the encryption and decryption keys are related to each other, rather than to a specific device. Therefore, Thompson teaches providing corresponding keys to two devices, rather than maintaining a crypto key *uniquely associated* with an implantable medical device.

Further, Griffiths shows authenticating electronic devices, such as a desktop computer, workstation, or handheld computing device using prior authentication data, but fails to specifically show an implantable medical device for which a uniquely associated crypto key is maintained. Therefore, Griffiths does not remedy the shortcomings of Thompson.

Claim 60 recites a short range interface device configured to provide communication with an implantable medical device by authenticating access to a securely maintained crypto key using a short range interface and an external device configured to commence a data exchange session with the implantable

medical device via a long range interface upon successful access authentication, and to transact the data exchange session using the crypto key. Claim 69 recites maintaining a short range interface device comprising providing communication with an implantable medical device and authenticating access to a securely maintained crypto key using a short range interface; and maintaining an external device comprising commencing a data exchange session with the implantable medical device via a long range interface upon successful access authentication and transacting the data exchange session using the crypto key. Claim 78 recites means for maintaining a short range interface device comprising means for providing communication with an implantable medical device and means for authenticating access to a securely maintained crypto key using a short range interface; and means for maintaining an external device comprising means for commencing a data exchange session with the implantable medical device via a long range interface upon successful access authentication and means for transacting the data exchange session by accessing patient health information stored on the implantable medical device using the crypto key. Applicant cannot find initiating a short range interface by a device and further initiating a long range interface between two different devices.

In contrast to the claimed subject matter, Griffiths discloses authenticating devices over a short-range wireless link and later, authenticating the same devices over an alternative communication link (Griffiths, Abstract). A first and second device are initially authenticated by exchanging authentication information via a short range wireless link (Griffiths, Col. 3, lines 44-48). When the devices move beyond the short range wireless link, authentication can be re-established when the first device establishes the alternative link to the second device (Griffiths, Col. 4, lines 16-28). After the alternative link is established, the second device initiates the exchange of authentication information (Griffiths, Col. 4, lines 34-37). If the keys of the authentication information match, the devices are authenticated and communication can occur (Griffiths, Col. 4, lines 7-39). However, the communication fails to occur when the devices are not first, successfully authenticated over the short-range link (Griffiths, Col. 4, lines 50-

55). Thus, in Griffiths, an initial authentication is performed between two devices and re-authentication occurs between the same two devices only when the initial authentication is successful. Accordingly, Griffiths fails to support communication between more than two devices when each of the devices has not been *initially* authenticated over a short range wireless link with the other devices. Therefore, Griffiths teaches initiating a short range wireless link and an alternative link between the *same two devices*, rather than initiating a short range interface to access a crypto key by a short range interface device and further initiating a long range interface between an external device and an implantable medical device.

Further, Thompson shows variably encrypting data on a device and transmitting the encrypted data, but fails to show initiating a short range interface by a short range interface device and initiating a long range interface between an external device and an implantable medical device. Therefore, Thompson does not remedy the shortcomings of Griffiths.

Moreover, the Thompson and Griffiths references lack a motivation to combine. "The motivation to combine may be implicit and may be found in the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved." Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co., 464 F.3d 1356, 1366 (Fed. Cir. 2006). Thompson teaches a variable encryption scheme for transmitting data to multiple devices (Thompson, Abstract; Col. 3, lines 23-25; and Col. 5, lines 41-43). A key source provides a first device, such as a programmer, and a second device, such as a clinician computer, with corresponding crypto keys (Thompson, Col. 8, lines 48-50). Upon receipt, the programmer encrypts sensitive data for transmitting to the clinician computer, where decryption occurs. Only one communication session occurs between the programmer and the clinician computer, in contrast to Griffiths. Griffiths teaches authenticating a communication between two devices over a primary link and then, reusing the authentication information to initiate another communication between the same two devices over a secondary link (Griffiths, Col. 2, lines 6-8; Col. 3, lines 51-56).

Thompson teaches transmitting data from one device to another using a single communication session. In contrast, Griffiths teaches initiating multiple communication sessions between two devices. Combining the teachings of Griffiths with Thompson would modify Thompson to require first, authentication over a short range wireless link prior to transmitting the encrypted data and second, a further communication over an alternative communication link. Also, Thompson focuses on solving a need for reducing large amounts of bandwidth required for high levels of data encryption, while, Griffiths focuses on solving a need for allowing two devices to authenticate a shared link outside predetermined authentication bounds, such as 100 meters for Bluetooth links. Thus, based on differences in the subject matter and the problems solved, one skilled in the art would not be motivated to combine the references. Accordingly, a teaching, suggestion, or motivation to combine Thompson and Griffiths has not been shown.

For the reasons described above, the combination of Thompson and Griffiths fails to render independent Claims 1, 17, and 34 obvious. Claims 3-10, 17-20, and 27-29 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 32-39, 46-49, and 56-58 are dependent upon Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 61 and 68 are dependent upon Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 70 and 77 are dependent upon Claim 69 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson, Griffiths, and Lee

Claims 79-81 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson, in view of Griffiths, and further in view of U.S. Patent No. 6,442,432, to Lee. Applicant traverses.

The examiner bears the initial burden of factually supporting any *prima*

facie conclusion of obviousness, which includes a clear articulation of the reasons or rationale why the claimed invention would have been obvious. MPEP 2142. Exemplary rationales to support a conclusion of obviousness are listed in MPEP 2143, although the list is not all-inclusive.

The claims appear to be rejected under the rationale outlining combining prior art elements according to known methods to yield predicable results, which includes *inter alia* "a finding that the prior art included each element claimed, although not necessarily in a single prior art reference, with the only difference between the claimed invention and the prior art being the lack of actual combination of the elements in a single prior art reference." MPEP 2143(A). If any of the findings cannot be made, this rational cannot be used to support a conclusion that the claim would have been obvious. *Id.*

Griffiths and Thompson have been described in detail above. Lee discloses providing data from an implantable medical device to distributed clinicians via an interface medical device (Lee, Abstract). A patient with an implantable medical device situates himself in proximity of the interface medical unit to allow the telemetry capabilities of the medical unit to obtain data (Lee, Col. 13, Lines 40-44). Once the interface medical device receives the data, an operator facilitates communication with remote medical devices and remote data communication devices via a central network (Lee, Col. 13, line 54 through page 14, line 2).

More specifically, the interface medical unit communicates with the implantable medical device through telemetry, while the interface medical unit in turn communicates with the medical devices, data communication devices, central collaboration computer, and export server through a network connection, such as a local area network or wireless area network (Lee, Col. 10, lines 43-61 and Col. 11, lines 25-44). The interface medical unit acts as a go-between for the implantable medical device and the network accessible devices. Thus, the remote medical devices and data communication devices only receive data from the implantable medical device via the interface medical device. The transfer of data includes a single communication during which the data is sent from the

implantable medical device to the interface medical device through radio frequency or proximity of the implantable medical device and interface medical device (Lee, Col. 11, lines 11-24).

The Thompson-Griffiths-Lee combination fails to teach each and every element of the claims. Claim 79 recites a secure external device configured to request the crypto key from the secure server device via a secure short range connection based on the identification of and authentication to access the implantable medical device, to receive the crypto key, to commence a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication, and to transact the data exchange session using the crypto key. Claim 80 recites maintaining a secure external device comprising requesting the crypto key from the secure server via a secure short range connection based on the identification of and authentication to access the implantable medical device . . . and commencing a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication transacting the data exchange session using the crypto key. Claim 81 recites means for maintaining a secure external device comprising means for requesting the crypto key from the secure server via a secure short range connection based on the identification of and authentication to access the implantable medical device . . . and means for commencing a data exchange session with the implantable medical device by means for transitioning to a long range interface upon successful access authentication.

Applicant cannot find such limitations in Griffiths. Griffiths discloses authenticating devices over a short-range wireless link and later, authenticating the same devices over an alternative communication link (Griffiths, Abstract). A first and second device are initially authenticated by exchanging authentication information via a short range wireless link (Griffiths, Col. 3, lines 44-48). When the devices move beyond the short range wireless link, authentication can be re-established when the first device establishes the alternative link to the second device (Griffiths, Col. 4, lines 16-28). After the alternative link is established, the

second device initiates the exchange of authentication information (Griffiths, Col. 4, lines 34-37). If the keys of the authentication information match, the devices are authenticated and communication can occur (Griffiths, Col. 4, lines 7-39). However, the communication fails to occur when the devices are not first, successfully authenticated over the short-range link (Griffiths, Col. 4, lines 50-55). Thus, in Griffiths, an initial authentication is performed between two devices and re-authentication occurs between the same two devices only when the initial authentication is successful. Accordingly, Griffiths fails to support communication between more than two devices when each of the devices has not been *initially* authenticated over a short range wireless link with the other devices. Therefore, Griffiths teaches initiating a short range wireless link and an alternative link between the *same two devices*, rather than maintaining a secure external device for requesting a crypto key from a secure server device via a secure short range connection and for commencing a data exchange session with an implantable medical device by transitioning to a long range interface.

Further, Thompson shows variably encrypting data on a device and transmitting the encrypted data, but fails to show requesting by a secure external device, a crypto key from a secure server device via a secure short range connection and commencing a data exchange session with an implantable medical device by transitioning to a long range interface. Even further, Lee shows a single communication with an implantable medical device to transfer data, but fails to show a secure short range connection for requesting by a secure external device, a crypto key from a secure server device, and a long range interface for commencing a data exchange session with an implantable medical device. Therefore, Thompson and Lee fail to remedy the shortcomings of Griffiths.

Further, the Thompson and Griffiths references lack a motivation to combine. "The motivation to combine may be implicit and may be found in the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved." Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co., 464 F.3d 1356, 1366 (Fed. Cir. 2006). Thompson teaches a variable encryption scheme for transmitting data to multiple devices (Thompson,

Abstract; Col. 3, lines 23-25; and Col. 5, lines 41-43). A key source provides a first device, such as a programmer, and a second device, such as a clinician computer, with corresponding crypto keys (Thompson, Col. 8, lines 48-50). Upon receipt, the programmer encrypts sensitive data for transmitting to the clinician computer, where decryption occurs. Only one communication session occurs between the programmer and the clinician computer, in contrast to Griffiths. Griffiths teaches authenticating a communication between two devices over a primary link and then, reusing the authentication information to initiate another communication between the same two devices over a secondary link (Griffiths, Col. 2, lines 6-8; Col. 3, lines 51-56).

The Thompson and Griffiths references differ at least because Thompson teaches transmitting data from one device to another using a single communication session. In contrast, Griffiths teaches initiating multiple communication sessions between two devices. Combining the teachings of Griffiths with Thompson would modify Thompson to require first, authentication over a short range wireless link prior to transmitting the encrypted data and second, a further communication over an alternative communication link. Also, Thompson focuses on solving a need for reducing large amounts of bandwidth required for high levels of data encryption, while, Griffiths focuses on solving a need for allowing two devices to authenticate a shared link outside predetermined authentication bounds, such as 100 meters for Bluetooth links. Thus, based on differences in the subject matter and the problems solved, one skilled in the art would not be motivated to combine the references. The addition of Lee to the Thompson-Griffiths combination does no more the make the Thompson and Griffiths closer related. Accordingly, a teaching, suggestion, or motivation to combine Thompson, Griffiths, and Lee has not been shown.

Therefore, the combination of Thompson, Griffiths, and Lee fails to render independent Claims 79-81 obvious. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson, Griffiths, and Eckmiller

Claims 11-16, 40-45, 62, 63, 65-67, 71, 72, and 74-76 stand rejected under

35 U.S.C. § 103(a) as being obvious over Thompson, in view of Griffiths, and further in view of U.S. Patent No. 6,493,587, to Eckmiller et al. ("Eckmiller"). Applicant traverses.

Adding the teachings of Eckmiller to the teachings of the Thompson and Griffiths combination introduces further functionality. However, as discussed above, the Thompson-Griffiths combination fails to render Claims 1, 30, 60, and 69 obvious, and the addition of Eckmiller does no more to support an obviousness rejection of Claims 11-16, 40-45, 62, 63, 65-67, 71, 72, and 74-76. Claims 11-16 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 40-45 are dependent upon Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 62, 63, 65-67 are dependent upon Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 71, 72, and 74-76 are dependent upon Claim 69 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson, Griffiths, and Wheeler

Claims 21-26, 50-55, 64 and 73 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson, in view of Griffiths, and further in view of U.S. Patent Application Publication No. 2002/0016913, to Wheeler et al. ("Wheeler"). Applicant traverses.

Adding the teachings of Wheeler to the teachings of the Thompson and Griffiths combination introduces further functionality. However, as discussed above, the Thompson-Griffiths combination fails to render Claims 1, 30, 60, and 69 obvious, and the addition of Wheeler does no more to support an obviousness rejection of Claims 21-26, 50-55, 64 and 73. Claims 21-26 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 50-55 are dependent upon Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 64 is dependent upon Claim 60 and is patentable

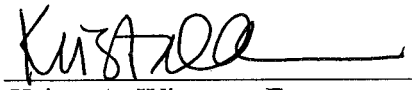
for the above-stated reasons, and as further distinguished by the limitations therein. Claim 73 is dependent upon Claim 69 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Claims 1, 3-30, and 32-81 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested. Reconsideration of the claims, withdrawal of the finality of the Office action, and a Notice of Allowance are earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: November 26, 2008

By: 
Krista A. Wittman, Esq.
Reg. No. 59,594

Cascadia Intellectual Property
500 Union Street, Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999